UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/871,152	05/31/2001	Carmi David Gressel	6727/0J419	7436

7590 04/10/2003

DARBY & DARBY P.C.
805 Third Avenue
New York, NY 10022

EXAMINER	
CAPUTO, LISA M	
ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 04/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/871,152	Applicant(s) GRESSEL ET AL.	
	Examiner Lisa M Caputo	Art Unit 2876	

-- The MAILING DATE of this communication appears on th cover she t with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-48 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-48 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 31 May 2001 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Israel on 13 December 2000. It is noted, however, that applicant has not filed a certified copy of the Israel application as required by 35 U.S.C. 119(b).

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: Page 12 line 20 references numbers 995 and 998 which do not appear in the Figures.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: Reference number 1600 is on Figure 6 but is not in the specification.

A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

4. The disclosure is objected to because of the following informalities:

Regarding page 3, line 10: Replace "applicatio" with --application--.

Regarding page 4 line 31 (and other occurrences throughout specification where grammatically appropriate): Replace "an" with --and--.

Regarding Page 12, lines 13-17: Replace "Security logic, 990," with --Security logic, 940,-- and "Control and Test Registers, 940," to --Control and Test Registers, 990,-- so that they are references according to Figure 3.

Regarding pages 12-14: Please ensure that all references numbers are accounted for and correct for Figure 4.

Appropriate correction is required.

Claim Objections

5. Claims 8, 14, 16, 18, 20-22, 24-26, 28, 30-41, 42, and 44 are objected to because of the following informalities:

Regarding claim 8, please add another clause/limitation to the claim as it seems as though the statement is incomplete.

Regarding claims 14,16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38-40, 42, and 44, "A method" should be replace with --A system-- so as to have proper dependency from claim 1, which is a system.

Regarding claims 20-21, there is no antecedent base for the "feature matrix" in claims 1 or 5. It seems as though claims 20-21 should be dependent on claims 18-19, respectively.

Regarding claims 24-25 and 40-41, please place a period on the end of these claims so that proper grammatical form is kept.

Regarding claims 30-39, there is no antecedent basis for "the circuit" in claims 1 or 5.

Regarding claims 38-39, replace "A method according to claims 1" with --A method according to claim 1--.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 1-5, 7-9, 13-31, and 34-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lang (U.S. Patent No. 5,065,429) in view of Drupsteen et al. (U.S. Patent No. 6,249,869, from hereinafter "Drupsteen").

Lang teaches a method and apparatus for protecting material on storage media. Lang discloses a method and apparatus for granting selected access to material such as data and databases, messages and other textual information, graphs, tables, maps, facsimiles (FAX) of all manner of transmitted materials (as recited in claims 14-15 of the instant application), audio such as speech and music (as recited in claims 22-25 of the instant application), video, images (as recited in claims 16-17 of the instant application), and photographs, provided on storage media utilizing information encoded in the storage media (the system is able to authenticate the validity and integrity of multi-origin data files as recited in claims 40-41 of the instant application). The storage media are included in one or more reading devices associated with a computer. A storage accessing device, such as a smart card (as recited in claims 30-31 of the instant application; in addition, due to the multiple implementations of the databases the smart card can hold financial data such as debit or credit information or flight information such as flight schedule as recited in claims 47-48 of the instant application), is used in conjuction with the computer to determine whether access to a particular user to specific storage media is granted. The storage media can be sub-divided (sub-modules as recited in claim 2 of the instant application) into a plurality of logical zones and access to all or a portion of the material on the storage media is granted based upon the logical zones to which the user is allowed access. Information provided on the storage media would include an index table listing the security identification code, the logical zones to which a particular user is assigned as well as a personal security key used in conjunction with a personal security key provided in the smart card. The interaction

between the user's personal accessing device and the index table provided on the storage media determine if access is granted as well as access privileges accorded to the user (see abstract).

Lang discloses that the deficiencies of the prior art are overcome by the present invention which is directed to a method and system for granting complete or limited access to information stored in a storage medium or media utilizing information physically stored in the storage medium or media (as recited in claims 34-39 of the instant application). The particular storage medium or media are included in an appropriate reader which is connected to a standard personal computer, minicomputer, or a mainframe computer having a means for entering personal and system access data therein, such as a keyboard. The storage medium can be any permanent or erasable item such as an optical disk, a CD ROM, a WORM, a floppy disk, a disk pack, a smart card, an integrated circuit card, an optical card, as well as special items such as a BERNOULLI box disk, or any other type of storage medium. However, for simplicity sake, we shall describe the present invention with respect to a CD ROM storage medium. Additionally, a storage accessing device (used interchangeably herein with the following terms- personal accessing device and smart card) provided with an encrypted or non-encrypted personal security key as well as personal identification code is included to allow an individual access to the storage medium or media. Furthermore, for ease of understanding the present invention, we shall describe the storage accessing device with respect to a SMART card that does not require an electronic, optical, capacitive or magnetic reader to receive or transmit personal and system data. Initially,

when the CD ROM is mastered, the information storage portion of the CD ROM is broken up according to a predetermined classification system and stored in various logical zones, each of which contains a discrete set of databases or other material therein. There may be one or more logical zones recorded on the CD ROM (sub-modules as recited in claim 2 of the instant application). Users, based on their need to know, as well as the sensitivity of the material to be stored on the CD ROM, are accorded access privileges that correspond to previously designated logical zones. Based on an organization's or person's storage classification system, material are categorized and stored in the corresponding logical zones when the CD ROM is manufactured. Therefore, for each user being granted access privileges, a determination is made as to which logical zones each particular user would be allowed access. Based upon this determination, each user is assigned a particular zone access code (ZAC) which is translated into corresponding logical zones using an index table stored in the CD ROM. At the same time, paired to the ZAC, is a list of authorized system identification codes, each with its assigned unique personal security key (SK). Each authorized user is assigned a ZAC and a unique system identification code. For extremely secure applications, the intended user's biometric coded information (as recited in claims 18-21 of the instant application) can be paired with the personal security key. The ZAC, the system identification code, the personal security key code, plus the possible use of biometric coded information, as well as the logical zones assigned to the ZAC for each user or class of user, is included on the CD ROM in the form of an index table when it is manufactured. When an individual wishes to gain

access to the CD ROM, the user would correctly enter his particular personal identification code in the aforementioned smart card which would then display both the ZAC as well as the system identification code in either encrypted or non-encrypted form. The user, utilizing a keyboard, would enter this code into the computer which then compares the decrypted or encrypted codes obtained from both the smart card and CD ROM and if a match is obtained, would then verify that this particular system ID code is proper and that material this accessor seeks access to is stored on the storage medium or media. The computer then retrieves the paired personal security key (SK). The computer would then generate a random number which is displayed upon its screen to serve as a challenge to the personal accessing device (smart card). The user would input this random number into the smart card via its keypad. The smart card as well as the computer are provided with a particular encryption/decryption algorithm (alternately a security microprocessor chip). Both the computer and the smart card would simultaneously compute a response to the challenge code (random number) and this response is displayed on the smart card screen (control values as recited in claim 4 of the instant application). This displayed response is then entered into the computer through its keyboard to determine whether there is a match. If a match is shown to have occurred, the computer will then display all the logical zones and material names therein to which access privileges have been granted and allow the user access to these logical zones provided in the storage media (as recited in claims 42-45 of the instant application). Further, the system then releases the system security key (SSK) which is transferred to the information processing device's volatile random access memory

(RAM) or to the security microprocessor chip board installed in the information processing device. The system security key is used to decrypt all the encrypted material transferred from the CD ROM. The information processing device's copy of the system security key is destroyed when the information processing device loses its power or if said device concludes its CD ROM activities and is then used for other applications. Each CD ROM has its own system security key recorded on it which would be retrieved by the information processing device for use during search and retrieval activities when authorized user access is established. The CD ROM search and retrieval program can be stored either on items such as floppy disks to be used at the time of CD ROM operation, on the information processing device's permanent memory, or on the CD ROM. If a type of contact or contactless smart card (wireless communication device as recited in claim 46 of the instant application) is used which requires a non-human reader, the operation is very similar to the activities described above. The personal identification code (as recited in claim 9 of the instant application) can be entered via the computer keyboard or via a keypad on the card reader. The entry of the correct personal identification code enables the smart card to start transmission and the paired ZAC and system identification codes which are stored in the smart card microcomputer's EPROM or EEPROM are transmitted to the computer. Based on the transmitted ZAC, the index table on the storage media is searched to determine if there is a match. If the corresponding ZAC is not stored in the index table of the storage medium or media, a message is displayed on the computer screen that access will not be granted. If there is a match of the ZAC's, then the associated system identification

codes stored on the storage medium or media are accessed until an exact match is found. If no match is found, the accessor will not be granted access. If an exact match is found, the personal security key paired with the user's system identification code is retrieved by the computer and is used to operate upon a randomly computer generated number. At the same time, the random number is also transmitted to the smart card reader which inputs the number to the smart card. The authorized user's smart card has both an identical encryption/decryption algorithm or microprocessor chip (as recited in claims 7-8 of the instant application) and personal security key to that of the information processing device and the CD ROM. The smart card operates on the random number using its internally stored personal security key and transmits the result through the card reader to the computer (information processing device). The information processing device uses an encryption/decryption algorithm or microprocessor chip to compare the results of both operations upon the random number. If a match occurs, the accessor's authorized status is ascertained and the predetermined access privileges are granted. With respect to software program application, while prior art devices include verification routines provided on the storage media to protect access to the entire program, no prior art device, however, limits access to only a portion of this program, or access to one program from two or more stored programs. Additionally, access can be provided to one or more programs from a plurality of programs. To prevent unauthorized access, the storage accessing device can be programmed to permit only one download or a specific number of downloads of the portion of the program or one or more programs from a plurality of programs on the media allowed access by the user... The CD ROM or any

type of storage media which is utilized would operate in conjunction with retrieval software stored in a number of ways such as on the CD ROM or on the computer or information processing device non-volatile memory (as recited in claim 13 of the instant application). If it is stored on floppy disks or other reusable media, such as the computer's hard disk, it can be updated as necessary to detect and deactivate outdated, duplicated or lost personal accessing devices, such as smart cards, which are presented for system access. An added feature could be that if a reported lost smart card 12 was used to gain access, and the computer or information processing device 20 determined it was a lost smart card, a "killer" challenge code could be displayed, which when entered into the smart card would deactivate the device. (see Figures 1-4, col 2 line 18 to col 7 line 38). Hence, Lang teaches a system and method that insures authorized access to secured repositories of data and programs that comprises a first component that is operable to provide authorized access to repositories and to prevent other applications from utilizing or modifying applications (in a broad sense Lang teaches that there is a second component that is able to execute programs in the form of different access privileges but this is not specific).

Regarding claims 1 and 3-5, Lang fails to specifically teach that there is a second component that executes programs loaded in the repositories.

Drupsteen teaches an integrated circuit card and secure application module system. Drupsteen discloses that the object of the present invention is to provide an integrated circuit card having a memory organized in a directory and file structure and in which memory space is saved by reducing the overhead data on the integrated circuit

card per application. To obtain this object the present invention provides an integrated circuit card wherein at least part of the memory means comprises service data in file structures within one directory comprising a first file and a second file, service data being grouped together in service slots, any service slot being divided into a profile part and a data part, any profile part having a slot number, and being stored in the first file and comprising a unique application identifier and any data part being stored in the second file and comprising data relating to the service, the memory means storing at least one key to protect write access to the first and second files. By means of a memory on the integrated circuit card structured as defined above it is enough to store only one or two keys on the card which are common to several service applications. Thus, less overhead data relating to any of the service applications on the card is required and more service applications can be supported by the integrated circuit card. In one embodiment, at least one profile part also comprises data relating to an expiry date of the service slot concerned. Such data relating to an expiry date may be checked by the secure application module which is communicating with the integrated circuit card. If it is established that the date has already expired the service slot concerned is available to any other new service application. Thus, no complicated arrangements have to be provided for between the hardware provider, the provider of the software and the party who is providing the service to the user of the integrated circuit card. The availability of a service slot of which the expiry date has expired can be checked automatically. When there are different application providers of the software related to several services the service slots are preferably structured such that they comprise their

own profile part and their own data part, the profile parts being implemented as records of the first file and the data parts being implemented as records of the second file, the memory means storing a further key to protect access to the first file. In such a case these service slots may be called "generic service slots". However, when there is only one application provider of the software for several services, preferably the implemented service slots share one common profile part but any service slot comprises its own data part, the common profile part being implemented as one record of the first file and the data parts being implemented as separate records of the second file. These service slots may be called "dedicated service slots". In such a case, the first file only comprises one record, thus saving required memory space for the profile part data. The directory of the integrated circuit card may be extended by a third file such that at least one service slot comprises an additional data part in the third file for storing additional data. Some service applications need a lot of additional data which may be stored in such an additional data part.

The present invention also relates to a secure application module equipped to communicate with an integrated circuit card, provided with memory means storing service data relating to at least one service, wherein at least part of the memory means comprises service data in file structures within one directory, the directory comprising at least one file, the at least one file storing service data relating to one single service grouped together into: application/service definition data comprising a unique service identifier and data indicating a service type; at least two application counters for administrating the number of allocations and for generating a unique record transaction

number; a service sequence counter for generating a unique object number and administrating the number of created service objects; a service float for administrating the number of either issued or received value units and data relating to access rights defining service actions allowed to be performed by predefined terminals, and wherein the memory means comprises at least a first key and a second key for protecting any data communication with an integrated circuit card. The service definition data and the keys on the secure application module are used for the management of the service application, which was controlled by access tables on the integrated circuit card in the mechanisms according to the prior art. Thus, management control data is now stored on the secure application module instead of on the integrated circuit card. However, this is no serious disadvantage since the available memory space on the secure application module is less critical than on the integrated circuit card itself. Moreover, such a construction has several advantages... Since the available memory space in secure application modules is less critical than on integrated circuit cards the number of possible access rights may be rather large. Access rights may be defined in more ways than only read or write. In accordance with the invention access rights may relate to creating, erasing, increasing, decreasing, validating, marking, and verifying service slots on the integrated circuit card and to modifying additional data parts if present (preparing the application session to an initial state as recited in claims 26-29 of the instant application). These are only examples: other types of access rights may be implemented on the secure application module. In an alternative embodiment, the method defined above includes the following step prior to the step of checking

predetermined access rights in step a: reading out service data from the service slot and storing in the secure application module a predetermined data part of the data which has to remain unchanged; and by the step of carrying out step b. without changing the predetermined part of the data on the integrated circuit card (see Figures 1-9, col 1 line 49 to col 21 line 34).

In view of the teaching of Drupsteen, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ a parallel second component that actually allows for execution of the programs that access was gained to because it is favorable to not only be able to access information, but to also be able to execute programs if necessary (i.e. services and modifications) in order to have a comprehensive, efficient system.

8. Claims 6, 10-12, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lang as modified by Drupsteen and further in view of Mandelbaum et al. (U.S. Patent No. 5,544,246, from hereinafter "Mandelbaum"). The teachings of Lang as modified by Drupsteen have been discussed above.

Regarding claims 6 and 32-33, Lang/Drupsteen fail to specifically disclose a system operable in a mobile communication device.

Mandelbaum discloses that because encryption ensures secure communication, the smartcard's issuer/owner can have confidence in remote installation of services. Of course, the issuer/owner (i.e., Root) must first log in into the smartcard. A protocol for the log-in is presented in FIG. 3, and a protocol for service installation process is presented in FIG. 4. The physical, remote, connection that is possible with the

smartcard disclosed herein is shown in FIG. 8 (see Figures 3,4, and 8, col 7 lines 37-44).

In view of the teaching of Mandelbaum, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the system in a mobile communication device because it is favorable to be able to access and utilize data in remote locations so that a more efficient system is realized.

Regarding claims 10-12, Lang/Drupsteen fail to specifically disclose that public key encryption is used.

Mandelbaum teaches a smartcard adapted for a plurality of service providers and for remote installation of the same. Mandelbaum discloses that another difference between the operating system of FIG. 2 and that of a standard UNIX operating system is that the former includes an encryption key pair that is installed in a file owned by Root (e.g., in "filex" 13), and that key pair is unique to each smartcard. The pair includes a private key, f, that is kept secret by the smartcard, and a public key, g, that the smartcard does not care to keep secret. Of course, both keys are initially known to the smartcard's owner/issuer, who is also the Root user (i.e., super user) of the smartcard, but Root need not keep the private key (and probably would choose to destroy that knowledge). This pair of keys can also be "burned" into an appropriate memory, such as the memory containing Root's password, or included in the file that defines the root directory. More about public key encryption is found below (see Figure 2, col 5 lines 46-61).

In view of the teaching of Mandelbaum it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ public key encryption because it is well known in the art that public key encryption is an efficient and useful way to encode data so that the data remains secure.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ***Lisa M. Caputo*** whose telephone number is **(703) 308-8505**. The examiner can normally be reached between the hours of 8:30AM to 5:00PM Monday through Friday. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on 703-305-3503. The fax phone number for this Group is (703)308-7722, (703)308-7724, or (703)308-7382.

Communications via Internet e-mail regarding this application, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be used by the applicant and should be addressed to [**lisa.caputo@uspto.gov**].

All Internet e-mail communications will be made of record in the application file. PTO employees do not engage in Internet communications where there exists a possibility that sensitive information could be identified or exchanged unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. This is more clearly set forth in the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 308-0956.

LMC
April 4, 2003

DIANE I. LEE
PRIMARY EXAMINER